PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2005-020105**
(43)Date of publication of application : **20.01.2005**

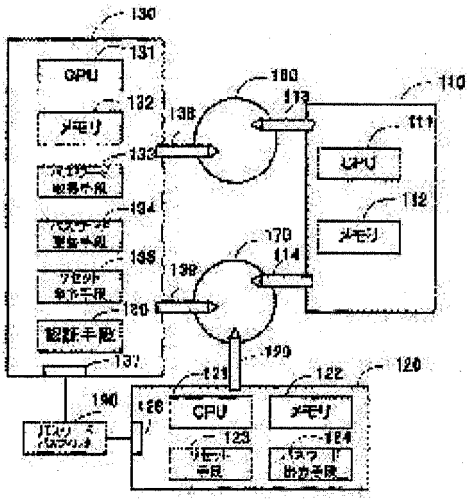
(51)Int.Cl. **H04L 9/32**
H04L 9/08

(21)Application number : **2003-178693**
(22)Date of filing : **23.06.2003**

(71)Applicant : **TAKANO NAOTO**
(72)Inventor : **TAKANO NAOTO**

(54) COMMUNICATION UNIT, INFORMATION COMMUNICATION SYSTEM, AND INFORMATION COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent leakage of data and falsification of data in a communication unit at a data transmission side or a communication unit at a data receiver side.
SOLUTION: The communication unit includes: an HD 170 for storing received encrypted data; an HD 160 for storing the transmitted encryption data; an information processing apparatus 110 for writing the received encrypted data in the HD 170 and for reading the encrypted data being a transmission object from the HD 160; an information processing apparatus 120 for reading the encrypted data stored in the HD 170 and decrypting the encrypted data by using a private key; an authentication means 130 for authenticating a password attached to the data decrypted by the information processing apparatus 120 and a password transmitted in advance; an information processing apparatus 130 for reading the encrypted data which are stored in the HD 170 and the password of which is confirmed for the coincidence with the password transmitted in advance by the authentication means 130, and writing the encrypted data being the transmission object to the HD 160; and a reset means 123 for resetting the encrypted data read by the information processing apparatus 120.



JP 2005-20105 A 2005.1.20

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-20105
(P2005-20105A)
(43)公開日　平成17年1月20日(2005.1.20)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/32	H04L	9/00	673A	5J104
H04L 9/08	H04L	9/00	601A	

審査請求 未請求　請求項の数 4　OL　（全 14 頁）

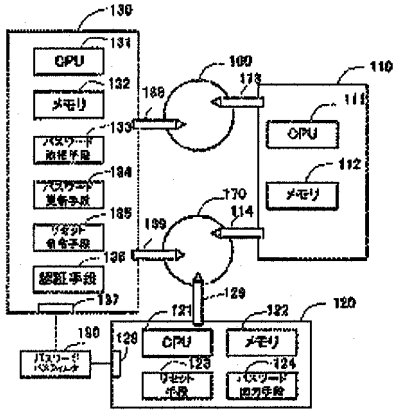
(21)出願番号　特願2003-178693(P2003-178693)
(22)出願日　平成15年6月23日(2003.6.23)

(71)出願人　300023730
▲高▼野　直人
千葉県千葉市花見川区畑町６６２番地の２１４
(74)代理人　100092048
弁理士　沢田　雅男
(72)発明者　高野　直人
千葉市花見川区畑町６６２－２１４

Fターム(参考)　5J104 AA07 KA01 NA05 PA07

(54)【発明の名称】通信ユニット、情報通信システムおよび情報通信方法

(57)【要約】
【課題】データの漏洩、改ざんを防止する。
【解決手段】受信した暗号化データを記憶するＨＤ１７０と、送信する暗号化データを記憶するＨＤ１６０と、受信した暗号化データをＨＤ１７０に書き込むとともに送信対象の暗号化データをＨＤ１６０から読み出す情報処理装置１１０と、ＨＤ１７０に記憶されている暗号化データを読み出して秘密キーを用いて暗号化データを復号化する情報処理装置１２０と、情報処理装置１２０によって復号化されたデータに付加されているパスワードとあらかじめ送ったパスワードとを認証する認証手段１３０と、認証手段１３０によってパスワード相互が一致したことが確認されたにＨＤ１７０に記憶されている暗号化データを読み出すとともに送信対象の暗号化データをＨＤ１６０に書き込む情報処理装置１３０と、情報処理装置１２０によって読み出した暗号化データをリセットするリセット手段１２３とを備える。
【選択図】　図２



【特許請求の範囲】
【請求項１】
データを送受信するのに先立って、ネットワーク接続されている他の通信ユニットとの間で、データを暗号化するための公開キーを交換するとともに、
データの受信時には初回の当該データの受信前に前記他の通信ユニットに対して秘匿性が保持されるルートを通じて前記データに付加させるパスワードを送り、かつ当該他の通信ユニットに対して送信対象のデータに前記パスワードを付加してから自己の公開キーを用いて暗号化してなる暗号化データを作成するように促し、実際に当該他の通信ユニットから送信されてきた前記暗号化データを自己の公開キーに対応する秘密キーを用いて復号化を行い、
データの送信時には当該送信前に前記他の通信ユニットから秘匿性が保持されるルートを通じて送信されたパスワードを付加した送信対象のデータを当該他の通信ユニットの公開キーを用いて暗号化することによって作成した暗号化データを前記他の通信ユニットに対して送信する通信ユニットであって、
前記他の通信ユニットから送信された暗号化データを記憶する第１の記憶部と、
前記他の通信ユニットに送信する暗号化データを記憶する第２の記憶部と、
前記他の通信ユニットから送信された暗号化データを前記第１の記憶部に書き込むとともに前記他の通信ユニットに送信する暗号化データを前記第２の記憶部から読み出す第１の情報処理装置と、
前記第１の記憶部に記憶されている暗号化データを読み出して前記自己の秘密キーを用いて復号化する第２の情報処理装置と、
前記第２の情報処理装置によって復号化されたデータに付加されていたパスワードとあらかじめ前記他の通信ユニットに送ったパスワードとを認証する認証手段と、
前記認証手段によってパスワード相互の一致が確認されたときに前記第１の記憶部に記憶されている暗号化データを復号化したデータを取得するとともに前記他の通信ユニットへ送信する暗号化データを前記第２の記憶部に書き込む第３の情報処理装置とを備えることを特徴とする通信ユニット。
【請求項２】
前記認証手段は、ディスプレイ、プリンタ、スピーカ、前記パスワードをパスするフィルタのいずれかであることを特徴とする請求項１記載の通信ユニット。
【請求項３】
請求項１または２記載の通信ユニットを複数備え、当該通信ユニット相互をネットワークで接続してなる情報通信システム。
【請求項４】
データを送受信するのに先立って、ネットワーク接続されている通信ユニット間で、データを暗号化するための公開キーを交換するとともに、初回の当該データの送受信前にデータ送信先の通信ユニットからデータ送信元の通信ユニットに対して秘匿性が保持されるルートを通じて前記データに付加させるパスワードを送り、
前記データ送信元の通信ユニットで、前記パスワードを付加した送信対象のデータを前記データ送信先の通信ユニットの公開キーを用いて暗号化することによって作成した暗号化データを、前記データ送信先の通信ユニットに対して送信するとともに、
前記データ送信先の通信ユニットで、前記データ送信元の通信ユニットから送信されてきた暗号化データを自己の公開キーに対応する秘密キーを用いて復号化を行う情報通信方法であって、
前記データ送信元の通信ユニットは、
第１の情報処理装置によって、前記データ送信先の通信ユニットへ送信する暗号化データを第１の記憶部に書き込み、
前記ネットワークに直接接続している第２の情報処理装置によって、前記第１の記憶部に記憶してある暗号化データを読み出し、
前記データ送信先の通信ユニットは、

前記ネットワークに直接接続している第３の情報処理装置によって、前記データ送信元の通信ユニットから送信されてきた暗号化データを第２の記憶部に書き込み、
第４の情報処理装置によって、前記第２の記憶部に記憶してある暗号化データの復号化を行い、
前記第４の情報処理装置によって復号化されたデータに付加されていたパスワードとあらかじめ送っているパスワードとが一致した場合に、第５の情報処理装置によって、前記第２の記憶部に記憶されている暗号化データを復号化したデータを取得することを特徴とする情報通信方法。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

本発明は、通信ユニット、情報通信システムおよび情報通信方法に関し、特に、データを暗号化して送信する通信ユニット、情報通信システムおよび情報通信方法に関する。

【０００２】

【従来の技術】

従来、データ通信の際に、送信対象のデータの秘匿性を保持するために、データを送受信するのに先立って、ネットワーク接続されている他の通信ユニットとの間で、暗号化されたデータを復号化するための公開キーを交換しておき、データ送信側から暗号化したデータを送信し、データ受信側で送信されてきたデータを公開キーを用いて復号化していた。

【０００３】

このような手法を採用するデータ転送方法について、特許文献１に記載がある。特許文献１には、送信部は、相手側の通信装置の受信部に公開キーを配送する。そして、通信電文を、受信側の通信装置の公開キーにより暗号化処理して送出する。当該通信電文を受信した受信部は、当該通信電文を、当該受信側の通信装置の秘密キーにより復号化処理して解読を行う、と記載されている。

【０００４】

【特許文献１】

特開平０９－０９３２４０号公報

【発明が解決しようとする課題】

しかし、従来の技術では、データ送信側の通信ユニットとデータ受信側の通信ユニットとを結ぶネットワークではデータの秘匿性が保持されるものの、データ送信側の通信ユニットあるいはデータ受信側の通信ユニットでは、ハッキング等により、データの秘匿性が保持されず、データが漏洩する場合があった。また、漏洩したデータが改ざんされることもあった。

【０００５】

そこで、本発明は、データ送信側の通信ユニットあるいはデータ受信側の通信ユニットにおけるデータの漏洩、データの改ざんを防止することを課題とする。

【０００６】

【課題を解決するための手段】

上記課題を解決するために、本発明は、データを送受信するのに先立って、ネットワーク接続されている他の通信ユニットとの間で、データを暗号化するための公開キーを交換するとともに、データの受信時には初回の当該データの受信前に前記他の通信ユニットに対して秘匿性が保持されるルートを通じて前記データに付加させるパスワードを送り、かつ当該他の通信ユニットに対して送信対象のデータに前記パスワードを付加してから自己の公開キーを用いて暗号化してなる暗号化データを作成するように促し、実際に当該他の通信ユニットから送信されてきた前記暗号化データを自己の公開キーに対応する秘密キーを用いて復号化を行い、データの送信時には当該送信前に前記他の通信ユニットから秘匿性が保持されるルートを通じて送信されたパスワードを付加した送信対象のデータを当該他の通信ユニットの公開キーを用いて暗号化することによって作成した暗号化データを前記他の通信ユニットに対して送信する通信ユニットであって、前記他の通信ユニットから送

信された暗号化データを記憶する第１の記憶部と、前記他の通信ユニットに送信する暗号化データを記憶する第２の記憶部と、前記他の通信ユニットから送信された暗号化データを前記第１の記憶部に書き込むとともに前記他の通信ユニットに送信する暗号化データを前記第２の記憶部から読み出す第１の情報処理装置と、前記第１の記憶部に記憶されている暗号化データを読み出して前記自己の秘密キーを用いて復号化する第２の情報処理装置と、前記第２の情報処理装置によって復号化されたデータに付加されていたパスワードとあらかじめ前記他の通信ユニットに送ったパスワードとを認証する認証手段と、前記認証手段によってパスワード相互の一致が確認されたときに前記第１の記憶部に記憶されている暗号化データを復号化したデータを取得するとともに前記他の通信ユニットへ送信する暗号化データを前記第２の記憶部に書き込む第３の情報処理装置とを備える。

【０００７】

また、前記認証手段は、ディスプレイ、プリンタ、スピーカ、前記パスワードをパスするフィルタのいずれかである。

【０００８】

さらに、本発明の情報通信システムは、上記通信ユニットを複数備え、当該通信ユニット相互をネットワークで接続してなる。

【０００９】

さらにまた、本発明は、データを送受信するのに先立って、ネットワーク接続されている通信ユニット間で、データを暗号化するための公開キーを交換するとともに、初回の当該データの送受信前にデータ送信先の通信ユニットからデータ送信元の通信ユニットに対して秘匿性が保持されるルートを通じて前記データに付加させるパスワードを送り、前記データ送信元の通信ユニットで、前記パスワードを付加した送信対象のデータを前記データ送信先の通信ユニットの公開キーを用いて暗号化することによって作成した暗号化データを、前記データ送信先の通信ユニットに対して送信するとともに、前記データ送信先の通信ユニットで、前記データ送信元の通信ユニットから送信されてきた暗号化データを自己の公開キーに対応する秘密キーを用いて復号化を行う情報通信方法であって、前記データ送信元の通信ユニットは、第１の情報処理装置によって、前記データ送信先の通信ユニットへ送信する暗号化データを第１の記憶部に書き込み、前記ネットワークに直接接続している第２の情報処理装置によって、前記第１の記憶部に記憶してある暗号化データを読み出し、前記データ送信先の通信ユニットは、前記ネットワークに直接接続している第３の情報処理装置によって、前記データ送信元の通信ユニットから送信されてきた暗号化データを第２の記憶部に書き込み、第４の情報処理装置によって、前記第２の記憶部に記憶してある暗号化データの復号化を行い、前記第４の情報処理装置によって復号化されたデータに付加されていたパスワードとあらかじめ送っているパスワードとが一致した場合に、第５の情報処理装置によって、前記第２の記憶部に記憶されている暗号化データを復号化したデータを取得する。

【００１０】

【発明を実施するための形態】

以下、本発明を実施するための形態について、図面を参照して説明する。

【００１１】

（実施形態１）

図１は、本発明の実施形態１の情報通信システムの模式的な構成を示すブロック図である。

【００１２】

図１には、以下説明する通信ユニット１００と通信ユニット２００とが、インターネット、アナログ電話回線、ＩＳＤＮ電話回線、ＤＳＬ、ＣＡＴＶ、光ファイバ、ｅｔｈｅｒＮｅｔ、１０ＢＡＳＥ－Ｔ、１００ＢＡＳＥ－Ｔ、赤外線、無線などのネットワーク３００を通じて接続されており、相互にデータ通信を行えるようにしている。

【００１３】

また、情報処理装置１３０と情報処理装置１４０、１５０とは、互にデータの入出力を行

えるように、ローカルエリアネットワーク（以下、「ＬＡＮ」と称する。）１８０あるいはイントラネットなどによって接続されている。

【００１４】

通信ユニット１００側と通信ユニット２００側との間では、データを送受信するのに先立って、それぞれ、一対の公開キーと秘密キーとを作成する。公開キーはデータを暗号化する際に用い、秘密キーは暗号化されているデータを復号化する際に用いる。そして、相互に公開キーを交換してある。

【００１５】

通信ユニット１００、２００は、ともに、データ送信元となる場合には、送信対象のデータと後述するパスワードとを、相手方の公開キーを用いて暗号化することによって作成した暗号化データを、データ送信先である通信ユニット２００、１００に対して送信する。一方、通信ユニット１００、２００は、ともに、データ送信先となる場合には、通信ユニット２００、１００で通信ユニット１００、２００から送信された暗号化データを受信して、自己の秘密キーを用いて復号化を行う。こうして、ネットワーク３００上におけるデータの漏洩を防止している。

【００１６】

さらに、本実施形態では、たとえば通信ユニット１００から通信ユニット２００に対してデータを送信する場合には、通信ユニット２００から通信ユニット１００宛てに、秘匿性が保持されるルートを通じて送信対象のデータに付加させるパスワードを送るようにしている。

【００１７】

具体的には、初回のデータを送受信するのに先立って、パスワードをデータの受信側の通信ユニットからデータの送信側の通信ユニットに送っておくようにしている。秘匿性が保持されるルートには、たとえば記憶媒体を通じた郵送によるルート、ネットワーク３００およびこれ以外の電話線等のネットワークによるルートがある。

【００１８】

また、これに代えて、たとえば通信ユニット１００は、通信ユニット２００向けのパスワードを通信ユニット２００の公開鍵で施錠し、通信ユニット２００にメールすることでパスワードを通信ユニット２００へ送るようにしてもよく、さらには通信ユニット１００側でホームページを有している場合には、通信ユニット２００の公開鍵で施錠したパスワードを、そのホームページに掲載するようしてもよい。＜ｂ＞

＜／ｂ＞

【００１９】

通信ユニット１００は、以下説明する情報処理装置１１０～１３０と、ハードディスク（以下、「ＨＤ」と称する。）１６０、１７０と、パスワードパスフィルタ１９０とを有している。

【００２０】

情報処理装置１１０は、通信ユニット２００から送信された暗号化データをＨＤ１７０に書き込むとともに、通信ユニット２００への送信対象の暗号化データをＨＤ１６０から読み出すものである。

【００２１】

情報処理装置１２０は、ＨＤ１７０に記憶されている暗号化データを読み出して、その暗号化データを自己の秘密キーで復号化し、復号化したデータおよびパスワードをパスワードパスフィルタ１９０へ出力するものである。

【００２２】

情報処理装置１３０は、情報処理装置１２０によって読み出された暗号化データに付随するパスワードと予め通信ユニット２００へ送っているパスワードとの認証を行い、暗号化データの送信元が通信ユニット１００であるという確認をしたときに、ＨＤ１７０に記憶されているデータを読み出すとともに、通信ユニット２００への送信対象の暗号化データをＨＤ１６０に書き込むものである。

【００２３】
ＨＤ１６０は、通信ユニット２００宛てに送信する暗号化データを記憶するものである。
【００２４】
ＨＤ１７０は、通信ユニット２００から送信された暗号化データを記憶するものである。
【００２５】
なお、ＨＤ１６０、１７０は、記憶媒体としての例示であり、ＤＶＤ－ＲＡＭ、半導体ディスク等のような外部記憶装置と称される記憶媒体を用いるようにしてもよい。
【００２６】
パスワードパスフィルタ１９０は、パスワードの認証を情報処理装置１３０で行えるようにするために、パスワードだけを通し、他の属性のデータを通さないようするものである。パスワードパスフィルタ１９０は、情報処理装置１２０、１３０に設けられているたとえばプリンタポート、ＵＳＢポートに接続されている。
【００２７】
なお、パスワードパスフィルタ１９０に代えて、ディスプレイ、プリンタ、スピーカなどのように、通信ユニットのユーザに対してパスワードを可視、可聴等によって報知可能なものを備え、ユーザが目視等によってパスワードの認証を行うようにしてもよい。パスワードパスフィルタ１９０としてはたとえばキャラクタデータだけを通すキャラクタパスフィルタを用いることができる。
【００２８】
通信ユニット２００は、それぞれ情報処理装置１１０～１３０に相当する情報処理装置２１０～２３０と、ＨＤ１６０、１７０に相当するＨＤ２６０、２７０と、パスワードパスフィルタ１９０に相当するパスワードパスフィルタ２９０とを有している。
【００２９】
図２は、図１に示す通信ユニット１００の模式的な内部構成を示すブロック図である。なお、通信ユニット２００も通信ユニット１００と同様の構成としている。
【００３０】
図２に示すように、情報処理装置１３０は、以下説明するＣＰＵ１３１と、メモリ１３２と、パスワード受取手段１３３と、パスワード更新手段１３４と、リセット命令手段１３５と、認証手段１３６、ＵＳＢポート１３７と、第１ヘッド１３８と、第２ヘッド１３９とを備えている。
【００３１】
ＣＰＵ１３１は、ＨＤ１７０から読み出した暗号化データの復号化処理を含む、種々の演算を実行することにより情報処理装置１３０本体の動作の制御を司るものである。
【００３２】
メモリ１３２は、主としてＣＰＵ１３１で実行するプログラムやデータを格納してあるものである。
【００３３】
【００３４】
パスワード受取手段１３３は、情報処理装置１２０側から出力される、通信ユニット２００から送信された暗号化データに付随するパスワードを受け取るものである。
【００３５】
パスワード更新手段１３４は、通信ユニット２００に送信する暗号化データを、たとえば乱数等を用いて更新するものである。なお、パスワードの更新は、たとえば内部犯行、すなわち情報処理装置１３０本体を不正操作することなどによるパスワードの漏洩に対処するために、暗号化データの交換の度にあるいは定期的に行うようにしている。
【００３６】
リセット命令手段１３５は、第２ヘッド１３９によって、通信ユニット２００から送信された暗号化データ読み出した後に、情報処理装置１２０で読み出してある、通信ユニット２００からの暗号化データと復号化後のデータおよびパスワードとをリセットする、あるいは情報処理装置１２０をリブートするように命令するものである。

【００３７】
認証手段１３６は、あらかじめ通信ユニット２００に送っているパスワードとパスワード受取手段１３３によって入力したパスワードとが一致しているか否かの認証を行うものである。
【００３８】
ＵＳＢポート１３７は、既述のように、パスワードパスフィルタ１９０と情報処理装置１３０本体とを接続するポートである。
【００３９】
第１ヘッド１３８は、通信ユニット２００に送信する暗号化データをＨＤ１６０に書き込むことが可能なヘッドである。ＣＰＵ１３１からの命令に応じて、暗号化データの書き込み位置にシークされ、通信ユニット２００へ送信する暗号化データの書き込みが行われる。なお、第１ヘッド１３８は、ハード的に通信ユニット２００に送信する暗号化データをＨＤ１６０に書き込みする専用ヘッドとしてもよいし、汎用的なヘッドをソフト的に制御して通信ユニット２００に送信する暗号化データをＨＤ１６０に書き込む専用としてもよい。
【００４０】
第２ヘッド１３９は、通信ユニット２００から送信されＨＤ１７０に記憶されている暗号化データを消去することが可能または読み出しすることが可能なヘッドである。認証手段１３６によってパスワード相互が一致していると判定されたことを条件として、ＣＰＵ１３１からの命令に応じて、暗号化データの消去位置または読み出し位置にシークして、通信ユニット２００から送信された暗号化データの消去または読み出しが行われる。なお、第２ヘッド１３９は、通信ユニット２００から送信されＨＤ１７０に記憶されている暗号化データを消去または読み出しする専用ヘッドとしてもよいし、汎用的なヘッドをソフト的に制御して通信ユニット２００から送信されＨＤ１７０に記憶されている暗号化データの消去専用または読み出し専用としてもよい。
【００４１】
情報処理装置１１０は、以下説明するＣＰＵ１１１と、メモリ１１２と、第１ヘッド１１３と、第２ヘッド１１４とを備えている。
【００４２】
ＣＰＵ１１１は、種々の演算を実行することにより情報処理装置１１０本体の動作の制御を司るものである。
【００４３】
メモリ１１２は、主としてＣＰＵ１１１で実行するプログラムやデータを格納してあるものである。
【００４４】
第１ヘッド１１３は、ＨＤ１６０に記憶されている、通信ユニット２００に送信する暗号化データを読み出しすることが可能なヘッドである。ＣＰＵ１１１からの命令に応じて、暗号化データの読み出し位置にシークされ、通信ユニット２００へ送信する暗号化データの読み出しが行われる。
【００４５】
第２ヘッド１１４は、通信ユニット２００から送信された暗号化データをＨＤ１７０に書き込むことが可能なヘッドである。ＣＰＵ１１１からの命令に応じて、第２ヘッド１１４をデータの書き込み位置にシークされ、通信ユニット２００から送信された暗号化データの書き込みが行われる。
【００４６】
なお、第１ヘッド１１３、第２ヘッド１１４は、それぞれ第１ヘッド１３８、第２ヘッド１３９と同様に、ハード的に実現してもよい、ソフト的に実現してもよい。
【００４７】
情報処理装置１２０は、以下説明するＣＰＵ１２１と、メモリ１２２と、リセット手段１２３と、パスワード出力手段１２４と、プリンタポート１２８と、ヘッド１２９とを備え

ている。

【００４８】

ＣＰＵ１２１は、ＨＤ１７０から読み出した暗号化データの復号化処理を含む、種々の演算を実行することにより情報処理装置１２０本体の動作の制御を司るものである。

【００４９】

メモリ１２２は、主としてＣＰＵ１２１で実行するプログラムやデータを格納してあるものである。

【００５０】

リセット手段１２３は、リセット命令手段１３５からの命令に従って、ＨＤ１７０から読み出してある、通信ユニット２００からの暗号化データと復号化後のデータおよびパスワードとをリセットする、あるいは情報処理装置１２０本体をリブートするものである。なお、リセット手段１２３とリセット命令手段１３５とに代えて、情報処理装置１３０で暗号化データを取得したことを検知する検知手段と検知手段による検知に応じて情報処理装置１２０側で自発的に情報処理装置１２０本体をリブート等する手段とを備えるようにしてもよい。

【００５１】

パスワード出力手段１２４は、通信ユニット２００から送信された暗号化データに付随するパスワードを出力するためのものである。

【００５２】

プリンタポート１２８は、既述のように、パスワードパスフィルタ１９０と情報処理装置１２０本体とを接続するポートである。

【００５３】

ヘッド１２９は、通信ユニット２００から送信されＨＤ１７０に記憶されている暗号化データを読み出し可能なヘッドである。ＣＰＵ１２１からの命令に応じて、暗号化データの読み出し位置にシークされ、通信ユニット２００から送信された暗号化データの読み出しが行われる。ヘッド１２９による動作は、第１ヘッド１３８、第２ヘッド１３９等と同様に、ハード的に実現してもよい、ソフト的に実現してもよい。

【００５４】

なお、第１ヘッド１１３、ヘッド１２９は、それぞれ、数秒毎にＨＤ１６０、１７０にアクセスして、暗号化データが書き込まれているか否かを判定し、暗号化データが書き込まれている場合には、それを読み出すようにしている。あるいは、たとえば第２ヘッド１１４、第１ヘッド１３８による暗号化データの書き込み完了をトリガとして光を出射する光出射器と、この光出射器から出射される光を受光可能な位置に光入射器を備えるようにして、光入射器で光を検知したことを条件として第１ヘッド１１３、ヘッド１２９によって暗号化データを読み出すようにしている。または、第２ヘッド１１４、第１ヘッド１３８による暗号化データの書き込み完了をトリガとしてフラグが書き換えられるステータスレジスタを設け、第１ヘッド１１３、ヘッド１２９側で、数秒毎にステータスレジスタにアクセスすることによって、暗号化データが書き込まれているか否かを判定し、暗号化データが書き込まれている場合には、それを読み出すようにしている。

【００５５】

こうして、ＣＰＵ１１１、１３１相互を接続することなく、ＨＤ１６０、１７０の暗号化データの書き込み完了後に、暗号化データを読み出し可能としている。

【００５６】

図３は、図１、図２に示す情報通信システムの動作の説明図である。なお、ここでは、情報処理装置１５０から情報処理装置２４０に向けてデータを送信する場合を例に動作の説明を行う。太線で図示している接続線は、データの流れを示す。

【００５７】

まず、既述のように、通信ユニット１００、２００間で相互の公開キーを交換するとともに、通信ユニット２００から通信ユニット１００宛にパスワードを送信しておく。

【００５８】

この状態で、情報処理装置１５０は、送信対象のデータを情報処理装置１３０へＬＡＮ１８０を介して出力する。

【００５９】

情報処理装置１３０は、情報処理装置１５０から出力された送信対象のデータに、通信ユニット２００から得られたパスワードをＣＰＵ１３１等によって付加する。そして、これらを、通信ユニット２００側の公開キーを用いて暗号化することによって暗号化データを作成する。作成した暗号化データは、ＣＰＵ１３１、第１ヘッド１３８等を用いてＨＤ１６０に書き込む。

【００６０】

なお、２回目以降のデータの送受信の際には、上記パスワードを送信対象のデータに付加するか、パスワード更新手段１３４によって更新されたパスワードを送信対象のデータに付加することになる。

【００６１】

ちなみに、情報処理装置１４０、１５０側に、通信ユニット２００から送られたパスワードを出力しておくとともに、情報処理装置１４０、１５０側で通信ユニット２００側の公開キーを記憶しておき、情報処理装置１４０、１５０側で暗号化データを作成可能とし、暗号化データを情報処理装置１４０、１５０から情報処理装置１３０へ出力するようにしてもよい。

【００６２】

ここで、本実施形態では、第１ヘッド１１３は、ＨＤ１６０に定期的にアクセスして、暗号化データが書き込まれているか否かを判定しており、ここでは暗号化データをＨＤ１６０に書き込みを行ったので、この暗号化データが第１ヘッド１１３によって読み出される。そして、読み出された暗号化データは、図示しない送信手段およびネットワーク３００を通じて、通信ユニット１００側から通信ユニット２００側へと送信される。

【００６３】

通信ユニット２００側では、情報処理装置２１０によって、通信ユニット１００側からの暗号化データが受信され、ＨＤ２７０に書き込まれる。

【００６４】

つづいて、情報処理装置２２０は、ＨＤ２７０への暗号化データの書き込み完了を検知すると、この暗号化データを読み出す。読み出した暗号化データは、自己の秘密キーを用いて復号化する。こうして、情報処理装置１５０から送信されたデータおよびパスワードを取得する。ひきつづき、情報処理装置２２０は、取得したデータおよびパスワードを、プリンタポート１２８等を介してパスワードパスフィルタ２９０へ出力する。

【００６５】

パスワードパスフィルタ２９０は、情報処理装置２２０から出力されたデータおよびパスワードを入力すると、キャラクタデータ以外の属性のデータを除去することによって、パスワードを情報処理装置２３０へ出力する。

【００６６】

情報処理装置２３０は、パスワードパスフィルタ２９０から出力されたパスワードを入力すると、このパスワードとあらかじめ通信ユニット１００へ送ってあるパスワードとを認証手段１３６によって認証する。

【００６７】

認証の結果、パスワード相互が一致していない場合には、ＨＤ２７０に書き込まれている暗号化データは所要のものでなく、たとえばウィルスを含んでいる可能性もあるので、情報処理装置２３０は、ＨＤ２７０に記憶されている暗号化データをデリートするとともに、情報処理装置２２０に対してＨＤ２７０から読み出した暗号化データ等のデリート命令をする。なお、図示しない報知手段によって、暗号化データが所要のものでない旨を、通信ユニット２００のユーザに報知するようにしてもよい。

【００６８】

一方、パスワード相互が一致している場合には、ＨＤ２７０に書き込まれている暗号化デ

ータは所妥のものであるので、情報処理装置２３０は、この暗号化データをＨＤ２７０から読み出して、自己の秘密キーによって復号化する。

【００６９】

なお、情報処理装置２２０ですでに暗号化データが復号化されていることとＨＤ２７０で使用するチャネル数を３チャネルから２チャネルに減らせるということとを考慮して、パスワードパスフィルタ２９０を含むルートと並列に情報処理装置２２０、２３０間を直接接続可能な別ルートを設けておき、情報処理装置２３０は、パスワード相互が一致している場合にだけ物理的に別ルートを開通させ、情報処理装置２２０で復号化されたデータを別ルートを介して入力するようにしてもよい。こうすると、情報処理装置２３０にネットワーク３００の外部からの進入を防止しつつ、情報処理装置２３０で通信ユニット１００側からのデータを取得することができる。

【００７０】

その後、情報処理装置２３０は、ＬＡＮ２８０を通じて情報処理装置２４０宛に復号化済みのデータを出力する。それから、情報処理装置２２０に対して暗号化データ等をリセットするように命令する。さらに、パスワードを更新することによって、次のデータ通信の際に使用するパスワードを用意して、更新したパスワードと更新前のパスワードとを情報処理装置１３０へ送信しておく。

【００７１】

情報処理装置２２０は、情報処理装置２３０からの命令に従って、ＨＤ２７０から読み出した暗号化データ等をリセットして、次回、通信ユニット１００から送信されてくる暗号化データの入力を可能とする。

【００７２】

また、情報処理装置１３０は、更新前後のパスワードを受信すると、更新前のパスワードを更新後のパスワードに書き換え、次回からのデータの送信時には更新後のパスワードを付加するようにするとともに、次回からのデータの受信時の認証を行えるようにする。

【００７３】

以上説明したように、本実施形態では、通信ユニット１００、２００間で種々のデータの送受信をする際に、外部から情報処理装置１３０、２３０に対する進入を防止している。

【００７４】

（実施形態２）

本発明の実施形態２として、図１に示す情報通信システムを、会員制ホームページの維持・管理に用いる場合を例に説明する。この会員制ホームページには、ホームページの管理者側のＥメールアドレスが掲載されており、会員と管理者側との間でＥメールの送受信を行えるようにしている。

【００７５】

図１に示す情報通信システムを、たとえば会員制ホームページの維持・管理に用いる場合には、会員制ホームページのシステム管理者側と会員との間で公開キーの交換をし、会員制ホームページのシステム管理者から会員に対してパスワードを発送等しておく。

【００７６】

そして、会員制ホームページのシステム管理者側は、会員制ホームページに掲載する情報等を会員が閲覧可能とするために、その情報等を暗号化してから第１ヘッド１３８によりＨＤ１６０へ書込む。

【００７７】

このホームページを閲覧しようとする会員は、ネットワーク３００を介して通信ユニット１００にアクセスする。これにより、情報処理装置１１０ではＨＤ１６０に書き込まれている情報等を第１ヘッド１１３で読み出して、会員側へ送信する。会員は、自己の秘密キーを用いて、通信ユニット１００から送信されてきた情報等を復号化することによって、その情報等を閲覧可能とする。

【００７８】

この場合、第１ヘッド１１３は、読み出し専用ヘッドであるため、ＨＤ１６０に書き込ま

れている情報等が、会員を含む第三者、すなわち外部から改ざんされることはない。

【００７９】

また、会員制ホームページに掲載している情報処理装置１１０に付随するＥメールアドレス宛てに、会員からＥメールを送信しようとする場合には、通信ユニット１００側から発送されているパスワードを付加したＥメールの情報を通信ユニット１００の公開キーで暗号化して、ネットワーク３００を経由して通信ユニット１００へ送信する。

【００８０】

この後の処理は、実施形態１で説明したとおり、送信されてきたＥメールのＨＤ１７０への書き込みを情報処理装置１１０で行い、ＨＤ１７０に書き込みされているＥメールの復号化を情報処理装置１２０で行い、復号化されたパスワードと発送しているパスワードとの認証を情報処理装置１３０で行い、認証確認ができたことを条件としてＨＤ１７０に書き込みされているＥメールの復号化をたとえば情報処理装置１３０で行う。このため、Ｅメールの内容は外部に曝されることがないし、改ざんされることもない。

【００８１】

また、本実施形態では、会員制ホームページの維持・管理に用いる場合を例に説明したが、たとえば公共工事の入札をオンラインで行う場合にも適用できる。この場合にも、入札状況が外部に漏れることがないし、改ざんされることもない。

【００８２】

（実施形態３）

図４は、本発明の実施形態３の情報通信システムの模式的な構成を示すブロック図である。なお、図４において、図２に示す部分と同様の部分には同一符号を付している。

【００８３】

図４に示すように、本実施形態では、図１等に示すＨＤ１６０、１７０に代えてＨＤ２００を備えるとともに、第１ヘッド１３８および第２ヘッド１３９に代えてヘッド２１０を備え、第１ヘッド１１３および第２ヘッド１１４に代えてヘッド２２０を備えている。

【００８４】

ＨＤ２００は、ＨＤ１６０に相当する第１領域２０１と、ＨＤ１７０に相当する第２領域２０２とが形成されている。

【００８５】

ヘッド２１０は、第１領域２０１に情報の書き込みが可能であり、かつ第２領域２０２から情報の読み出しが可能なヘッドである。

【００８６】

ヘッド２２０は、第１領域２０１から情報の読み出しが可能であり、かつ第２領域２０２に情報の書き込みが可能なヘッドである。

【００８７】

ヘッド１２９は、第２領域２０２から情報の読み出しが可能なヘッドである。

【００８８】

なお、ヘッド２１０、２２０、１２９は、その専用機能をハード的に実現してもよいし、ソフト的に実現してもよい。

【００８９】

本実施形態では、ＨＤ２００とヘッド２１０、２２０とを備え、情報処理装置１１０、１３０でヘッド２１０、２２０に対して時間多重制御を行うことで、既述の効果を維持しつつ、部品数を減らすことによる情報通信システムの小型化・低廉化を実現している。

【００９０】

（実施形態４）

本発明の実施形態４では、実施形態３で説明したＨＤ２００に第１領域２０１と第２領域２０２とを形成することなく、実施形態１の情報通信システムと同様の効果を奏する情報通信システムについて説明する。

【００９１】

本実施形態の情報通信システムでは、ＨＤ２００に記憶されている全てのファイルに、各

ヘッド２１０、２２０、１２９で扱えるファイルを特定するためのフラグを、各ヘッド２１０、２２０、１２９がＨＤ２００にファイルを書き込む際に、割り当てるようにしている。

【００９２】

これらのフラグとしては、たとえばフラグＡ～Ｃを用意しておき、下記のように割り当てるようにしている。なお、用意するフラグの数は３つに限定されず、各ヘッド２１０、２２０、１２９で扱えるファイルの特定要件を細分化して、４つ以上としてもよい。

【００９３】

上記のように、ヘッド２２０は、フラグＡが割り当てられたファイルだけを読み出し可能である。なお、書き込みの際には、ファイルにフラグＢを割り当てる。

【００９４】

ヘッド２１０は、いずれのフラグが割り当てられたファイルであっても読み出し可能である。なお、書き込みの際には、ファイルにフラグＡ～Ｃのいずれであっても割り当て可能である。

【００９５】

さらに、ヘッド２１０は、既存のファイルに割り当てられているフラグの変更を行うことも可能であり、情報処理装置１１０はたとえばフラグＢを割り当ててから書き込みしたファイルを読み出して、再度ＨＤ２００に書き込みする際には、フラグＣを割り当ててから、ＨＤ２００に書き込むことができる。

【００９６】

ヘッド１２９は、フラグＣが割り当てられたファイルだけを読み出し可能である。

【００９７】

なお、ヘッド２１０、２２０、１２９は、その専用機能をハード的に実現してもよいし、ソフト的に実現してもよい。

【００９８】

本実施形態では、部品数の削減による情報通信システムの小型化・低廉化の実現のみならず、ＨＤ２００という汎用的なＨＤを備えることで、さらなる情報通信システムの低廉化を実現している。

【００９９】

以上、本発明の各実施形態では、複数の情報処理装置１１０～１３０等を含む情報通信システム１００、２００を例に説明したが、情報通信システム１００、２００は、たとえば半導体化して作り上げるようにしてもよい。

【０１００】

また、ＨＤ１６０、ＨＤ１７０、ＨＤ２６０、ＨＤ２７０、ＨＤ２００、とそれらの持つヘッドは既存の１ヘッドハードディスクに、複数の入出力チャネルを持つ例えば時間多重制御基盤を付加する事によってその専用機能を実現してもよい。

【０１０１】

【発明の効果】

以上説明したように、本発明によると、データ送信側の通信ユニットあるいはデータ受信側の通信ユニットに備える記憶部に、ネットワークを通じて送信されてきた情報が書き込まれた後には、その情報をネットワークに接続されている外部の通信ユニットから読み出しを行えないようにしているので、データの漏洩、データの改ざんを防止することができる。

【図面の簡単な説明】

【図１】本発明の実施形態１の情報通信システムの模式的な構成を示すブロック図である。

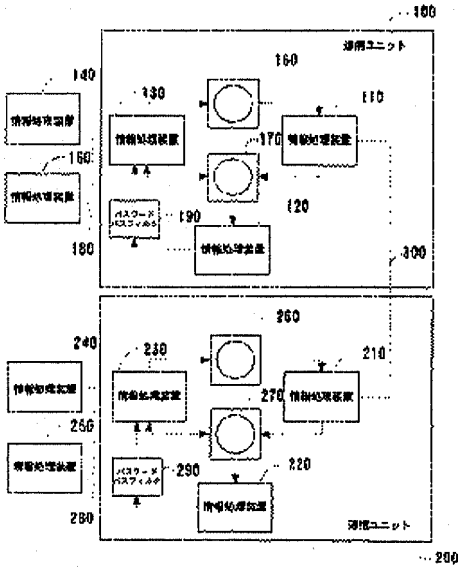
【図２】図１に示す通信ユニット１００の模式的な内部構成を示すブロック図である。

【図３】図１、図２に示す情報通信システムの動作の説明図である。

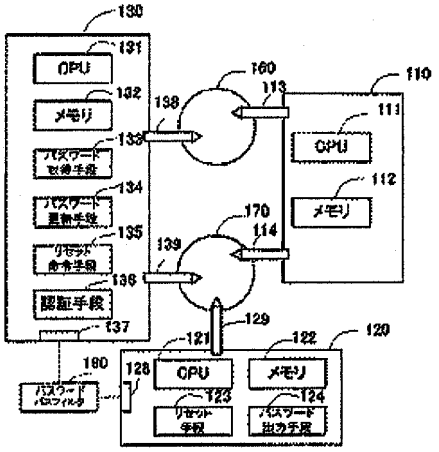
【図４】本発明の実施形態３の情報通信システムの模式的な構成を示すブロック図である。

【符号の説明】
１１０～１５０、２１０～２５０　情報処理装置
１６０、１７０、２６０、２７０　ＨＤ
１９０、２９０　パスワードパスフィルタ
１１１、１２１、１３１　ＣＰＵ
１１２、１２２、１３２　メモリ
１２３　リセット手段
１２４　パスワード出力手段
１２８　プリンタポート
１３３　パスワード受取手段
１３４　パスワード更新手段
１３５　リセット命令手段
１１３、１３８　第１ヘッド
１１４、１３９　第２ヘッド
１３６　認証手段
１３７　ＵＳＢポート

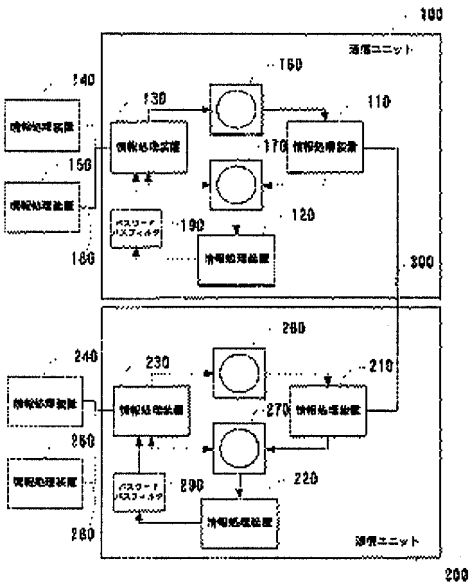
【図１】



【図２】



【図３】



【図４】